IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

updating said resident software with said available software if said resident software and said available software are ~~has~~ not ~~been~~ authenticated; ~~and~~

setting an authentication flag if said resident software is not authenticated but ~~and~~ said available software is authenticated; and

updating said resident software if said resident software is not authenticated but ~~and~~ said available software is authenticated.

2. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

updating said resident software with said available software if one of the following three conditions is met;

(1) said resident software and said available software are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.

3. (Previously Presented) The method of claim 2 wherein said determining

whether or not said resident software is authenticated comprises of:

determining whether or not an authentication flag has been set;

wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise

said resident software is determined to be unauthenticated.

4. (Previously Presented) The method of claim 3 wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

5. (Previously Presented) The method of claim 4 wherein said authentication flag is set by a service technician.

6. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of performing a direct authentication procedure on said resident software.

7. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

8. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

9 - 20. (Canceled).

21. (New) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for updating said resident software with said available software if said resident software and said available software are not authenticated;

means for setting an authentication flag if said resident software is not authenticated but said available software is authenticated; and

means for updating said resident software if said resident software is not authenticated but said available software is authenticated.

22. (New) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

means for updating said resident software with said available software if one of the following three conditions is met:

(1) said resident software and said available software are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.

23. (New) A computer-readable medium embodying instruction, which when executed by a processor, implement a method for configuration management for a computing device, the method comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

updating said resident software with said available software if said resident software and said available software are not authenticated;

setting an authentication flag if said resident software is not authenticated but said available software is authenticated; and

updating said resident software if said resident software is not authenticated but said available software is authenticated.

24. (New) A computer-readable medium embodying instruction, which when

executed by a processor, implement a method for configuration management for a computing device, the method comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

updating said resident software with said available software if one of the following three conditions is met:

(1) said resident software and said available software are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.